Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 27 gennaio 2020 – 4 CFU (la tesina vale 2 CFU)

SE NON HAI CONSEGNATO LA TESINA NON PUOI SOSTENERE QUESTO ESAME

Usa questa pagina per la brutta, staccala, non consegnarla.

Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 27 gennaio 2020 – 4 CFU (la tesina vale 2 CFU)

Usa questa pagina per la brutta, staccala, non consegnarla.

Cognome:_____ Nome: _____ Matricola:_____

Cybersecurity – 27 gennaio 2020 – 4 CFU (la tesina vale 2 CFU)

SE NON HAI CONSEGNATO LA TESINA NON PUOI SOSTENERE QUESTO ESAME

Tempo a disposizione: 60 minuti. Libri e appunti chiusi. Vietato comunicare con chiunque. Vietato l'uso di smartphone/watch, calcolatrici e affini.

1. **SQL injection.**
   1.1. Mostra un esempio di attacco SQL injection.

   1.2. Supponi di voler capire se un servizio web è vulnerabile ad SQL injection (nella sua forma più semplice), come fai a verificarlo?

   1.3. Cose suggerisci di fare per evitare che un servizio web abbia una tale vulnerabilità?

2. **Auditing.** Rispondi alle seguenti domande circa vari aspetti dell'auditing in ambito cybersecurity.
   2.1. Elenca tre azioni classificabili come auditing di sicurezza e descrivile brevemente.

   1.

   2.

   3.

   2.2. Che cosa è un SIEM? Che tipo di supporto può fornire nell'ambito dell'auditing?

2.3. Considera il framework ISO 27001. Qual è la sua relazione con il concetto di auditing?

3. Blockchain e Bitcoin.

3.1. Spiega che significa "consenso" nel contesto generale delle blockchain.

3.2. Spiega brevemente il consenso con proof of work e che significa che un nodo "accetta" un blocco.

3.3. Supponi di avere un client *leggero* per Bitcoin che non memorizza tutte le transazioni ma solo gli header dei blocchi. Il client leggero può richiedere una qualsiasi transazione ad un nodo che invece memorizza tutto. Come può essere certificata l'integrità della risposta?

4. Chiavi crittografiche. Rispondi brevemente a ciascuna domanda.

4.1. In cosa consiste il problema della distribuzione delle chiavi simmetriche? Come si risolve?

4.2. In cosa consiste il problema della identità associata alla chiave pubblica? Come si risolve?

4.3. Le chiavi "si deteriorano con l'uso e col tempo": spiega il **perché** e spiega il **rimedio**.

4.4. Definisci i concetti di chiave *di sessione* e *di autenticazione*. Che **precauzioni** si prendono nei due casi?

4.5. Che significa "chiave effimera" e a cosa serve?

4.6. Generazione di chiavi simmetriche: perché non si può usare un generatore di numeri casuali standard?

5. Autenticazione con password

5.1. Quali sono le principali problematiche di sicurezza relative alle password?

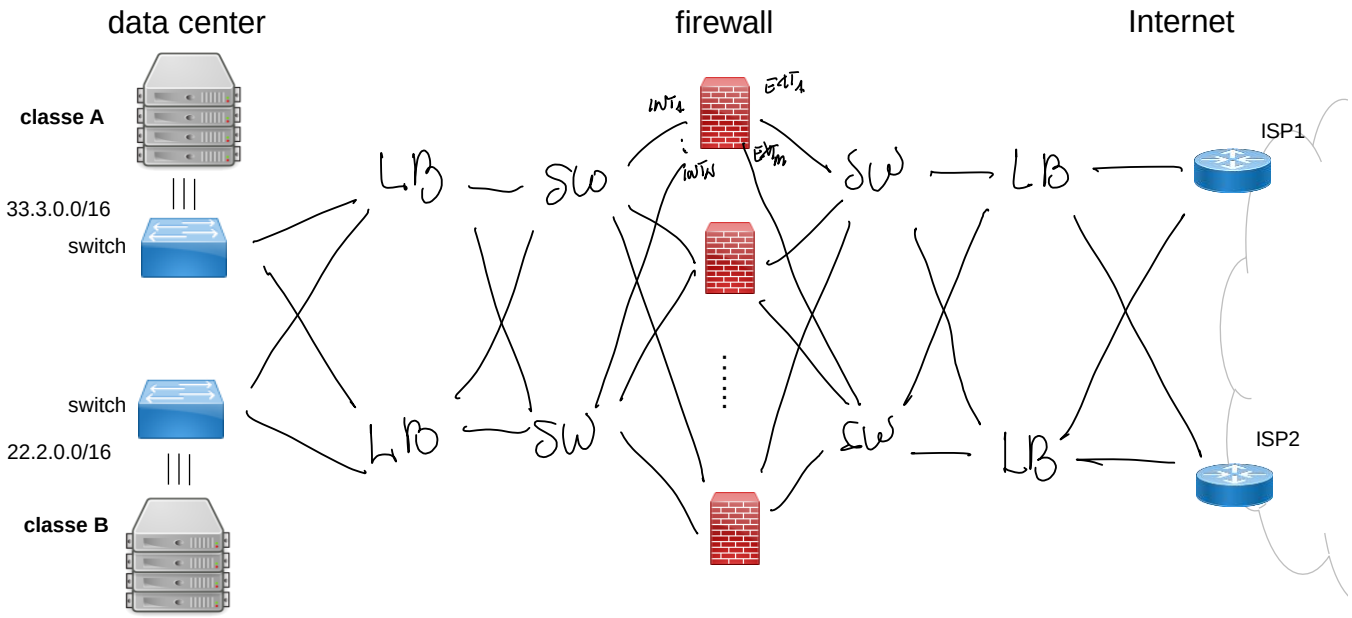
5.2. Che contromisure e tecniche conosci per ovviare ai problemi delle password? Per ciascuna contromisura o tecnica fornisci anche delle possibili criticità.

Cognome:_____ **Nome:** _____ **Matricola:**_____

Cybersecurity – 27 gennaio 2020 – 4 CFU (la tesina vale 2 CFU)

6. Firewalling nei data center.

Considera la rete in figura in cui sono indicati: un data center con due classi di server A e B con i loro indirizzi, i firewall per proteggere il datacenter e due ISP. I firewall mostrati non sono dotati di meccanismi autonomi di propagazione del loro stato delle connessioni.



6.1. Completa la figura aggiungendo collegamenti, switch e bilanciatori di carico in modo da soddisfare i seguenti requisiti.

- I firewall devono essere usati in modo che il carico sia bilanciato tra di essi.
- Non deve esistere alcun single-point-of-failure.

Scrivi in questo riquadro annotazioni che ritieni opportune circa le caratteristiche e le configurazioni degli apparati della rete ed eventuali protocolli di routing attivi.

- SU TUTTI GLI APPARATI DI LIVELLO 3 È ATTIVO OSPF
- I LB SONO COORDINATI PER INVIARE PACCHETTI DELLA STESSA CONNESSIONE ALLO STESSO FIREWALL. (VEDI SLIDES 27-37 DELLA PARTE SUI FIREWALLS)

6.2. Scrivi la configurazione di ciascuno dei firewall (dovrebbero essere tutte uguali) in modo da realizzare la seguente policy (dove tutto ciò che non è ammesso è negato).

- Classe A: ammesse richieste sulla porta 80 (http) da Internet.
- Classe B: ammesse richieste sulla porta 22 (ssh) da Internet e richieste arbitrarie verso Internet.

Usa preferibilmente la sintassi di iptables. Eventualmente aggiungi nel disegno dettagli come i nomi delle interfacce, se servono per la comprensibilità della configurazione.

Supponiamo che ciascun firewall abbia
- n interfacce verso il data center chiamate int_1... int_n ed
- m interfacce verso internet chiamate ext_1...ext_m.

la configurazione con la sintassi di netfilter è la seguente

```
:FORWARD DROP

per ogni i in 1..m le seguenti due regole
-A FORWARD -i ext_i -d 33.3.0.0/16 --dport 80 --state NEW -j ACCEPT
-A FORWARD -i ext_i -d 33.2.0.0/16 --dport 22 --state NEW -j ACCEPT

per ogni i in 1..n la seguente regola
-A FORWARD -i int_i --state NEW -j ACCEPT

e poi
-A FORWARD --state ESTABLISHED -j ACCEPT
```